http://www.univerself-project.eu/

http://www.etsi.org/

Unified Approach to Trust in Autonomic Networks and their Management

Laurent Ciavaglia
Alcatel-Lucent Bell Labs France
(On behalf of the UniverSelf consortium)

2nd ETSI Workshop on Future Network Technologies, session Autonomic Network Management, 27.SEP.2011, Sophia-Antipolis, France

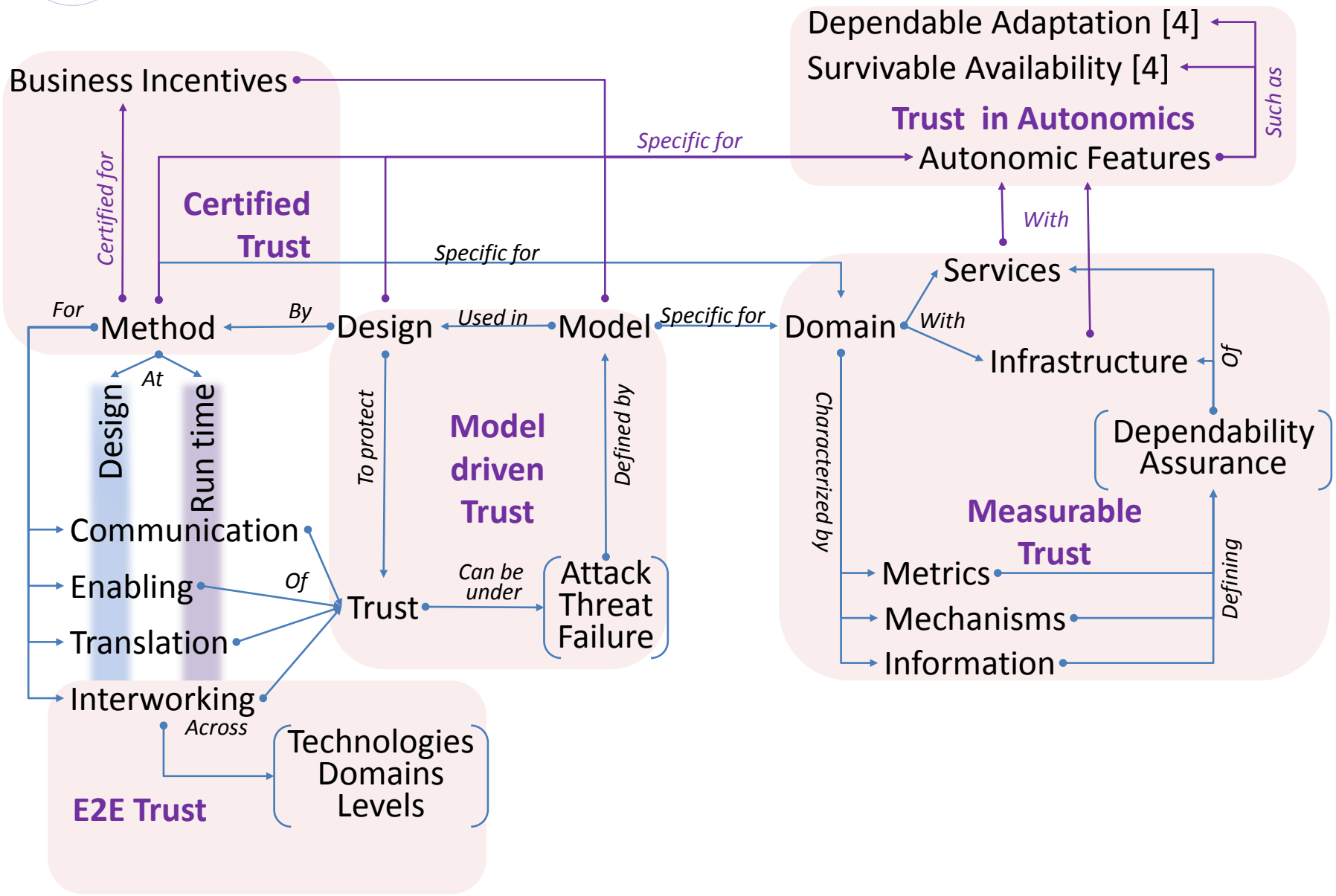
The Roadmap

"*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*"

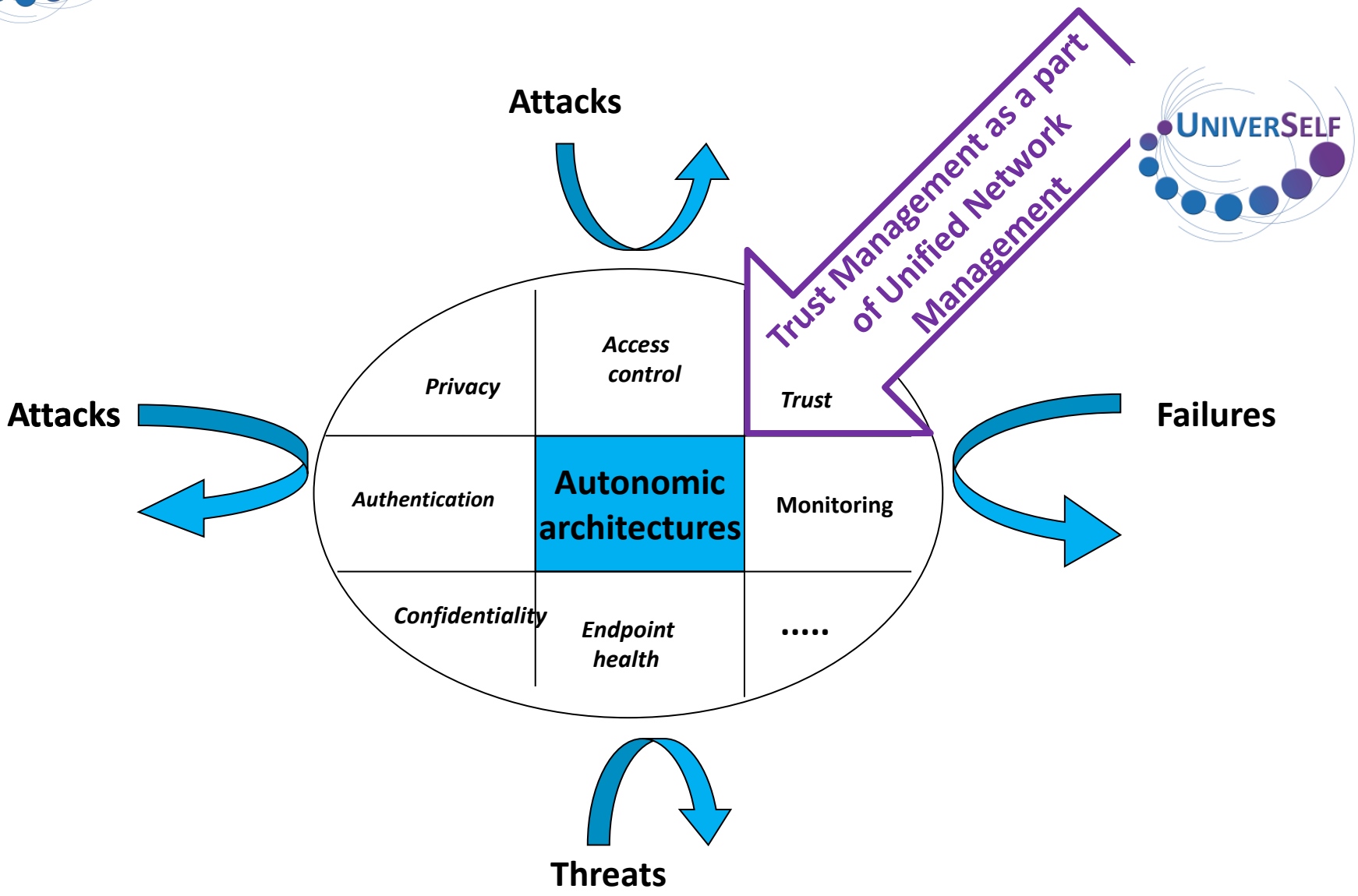
Virgil Gligor, University of Maryland, National Security Award 2006,
Invited talk at The 3rd Annual VoIP Security Workshop, Berlin, Fraunhofer FOKUS, 01.JUN.2006

- **Understanding trust issues arising from autonomics**
- **Innovation: Focus on Unified Management of (Autonomics + Trust in Autonomics)**
- **Autonomic-specific metrics**
- **Towards Certification of Autonomic features**
  - Certification model(s)
  - Process
  - Business Impacts
- **Towards Unified Trust + Management mechanisms**
  - Predicates-based trust
  - Design for trust
  - The Power of predicates
- **Actions in Standard bodies and UniverSelf plans**
- **Acknowledgements, References, Glossary**

Understanding Trust



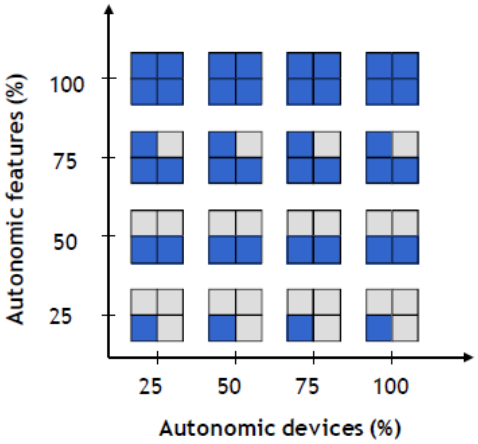
Innovation space

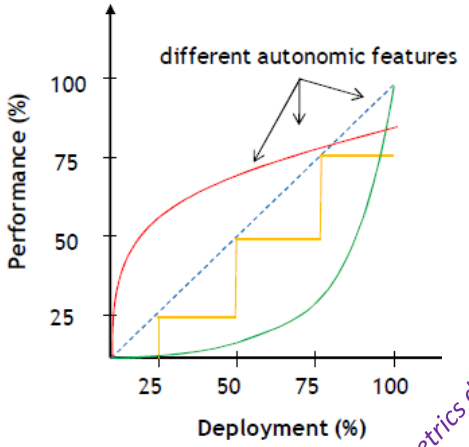


Source: Yacine Rebahi, Ranganai Chaparadza, "EFIPSANS Security Roadmap"

Autonomic-specific metrics

Step-by-step deployment of autonomic features shall not deteriorate the global **network performance** *Measured by*





Availability
Connectivity

One-way delay
One-way loss
Round-trip delay
Jitter
Loss patterns

Packet re-ordering
Link bandwidth
Packet duplication

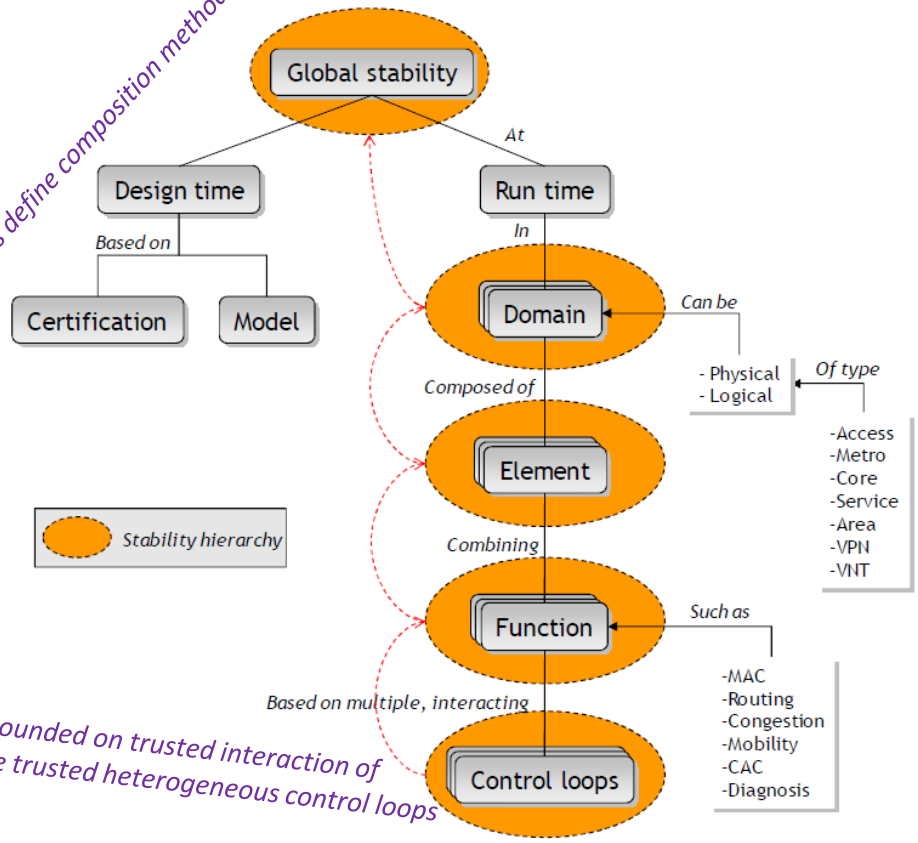
Metrics

Routing metrics
Service availability
Network device state

Possible metrics for **autonomic features**

- Autonomy level
- Learning ability
- Compatibility
- Adaptability
- Scalability
- Response time
- Dependability
- ...
- Stability

Standard metrics define composition method of

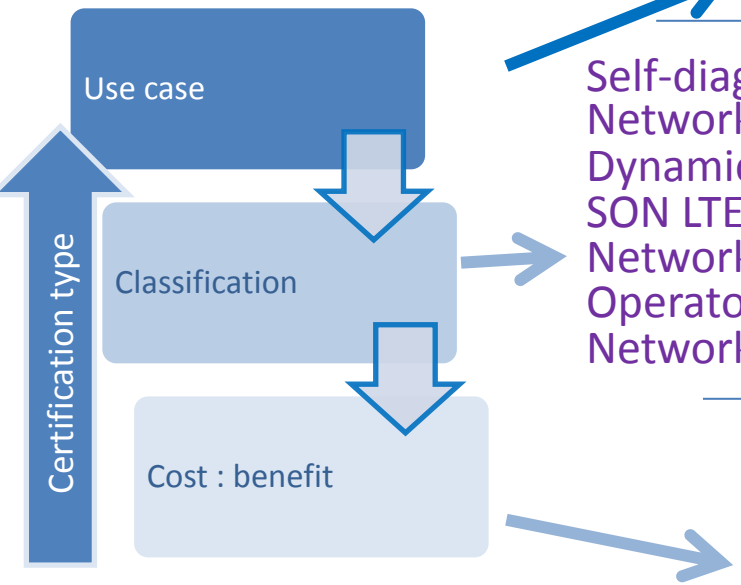


Grounded on trusted interaction of multiple trusted heterogeneous control loops

Source: Pedro B. Velloso, Laurent Ciavaglia "Composition of Well-known Metrics to Characterize Autonomic Networks", IEEE Network Magazine

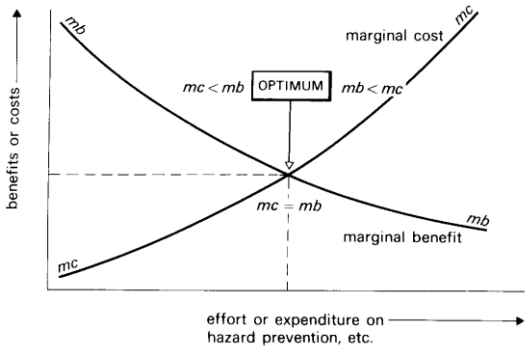
Certification models

- Certification of **systems, process, services**… à la **ISO**… à la **MEF**…
- Define the **type of certification** needed per particular use case according to the UniverSelf developed classification and performing the associated **Cost-Benefit analysis**;



Application domain

Self-diagnosis and -healing → IMS with VoIP and VPN services
Networks stability/performance
Dynamic virtualization/migration contents/servers in mobile access
SON LTE collaboration under operator-policies
Network-morphing
Operator-governed/E2E/autonomic/network& service management
Network and Service Governance



"The marginal benefit of increasing investment for a given adjustment (mb) represents demand, or willingness to pay; this decreases with increasing effort or expenditure on hazard prevention. Marginal cost (mc) represents supply. The optimum state exists when marginal costs and marginal benefits are equal."

Text/Picture credit: http://www.lancs.ac.uk/staff/gyaccp/hazards/chap6.htm

KPI Envelope

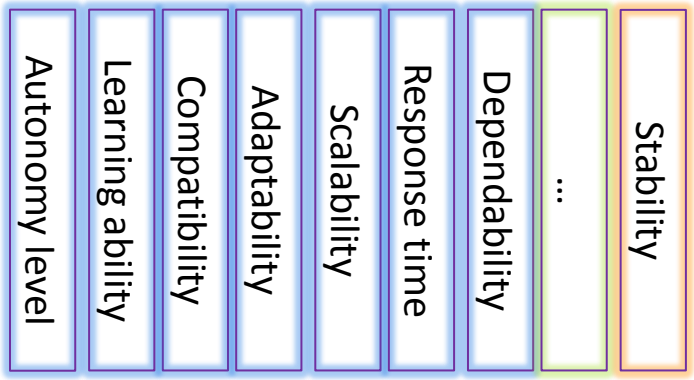
- The **KPI-based envelope** of process-correct adaptations of the system will be used in the trustworthiness evaluation of the system;
- the KPI-based envelope can include
  - point correctness criteria (such as scalability, stability, security, availability, reliability, consistency, response time, etc.) evaluated for various networking contexts
  - and their combinations to cater for statistically sound evaluation of process correctness;
  - these stationary criteria will be enriched by those assessing dynamic and transient properties (e.g. the rate of self-healing, convergence times, etc.);

The KPI-based envelope ensures dependable adaptations

Certification Process

- The **certification procedures** can be divided into the two clusters:
  - first, to assess the performance criteria, which will capture recommendations and best current practices of the usage of testbeds, simulations, and mathematical analysis related to the classes of use cases;
  - Second, defining autonomic criteria for autonomy certification, considering the trade-off between rigorous certification rules and flexibility to support new applications.

Open set of criteria



Business Impacts

- Must consider **potential business impacts** related to the newly introduced certification procedure.
- These might be related to:
  - the functional architecture,
  - value network,
  - cost and revenue structure or
  - the value proposition for the certified system under study.

Trust in Autonomics can be achieved via the use of **predicates**

The Approach

Focus is on structure (hierarchy) and functional blocks

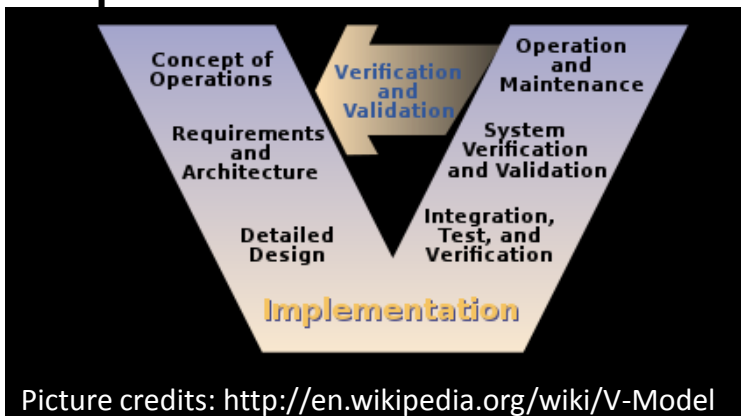
WP2

Design Phase

Behaviour is Pre-defined

Governed by Goal policies

Operational trust is to be build



Picture credits: http://en.wikipedia.org/wiki/V-Model

During the design

Define Trust Predicates

Verify Trust Predicates

Focus is on control loops and their interaction

WP3

Operation Phase

Behaviour is emergent

Governed by Goal policies

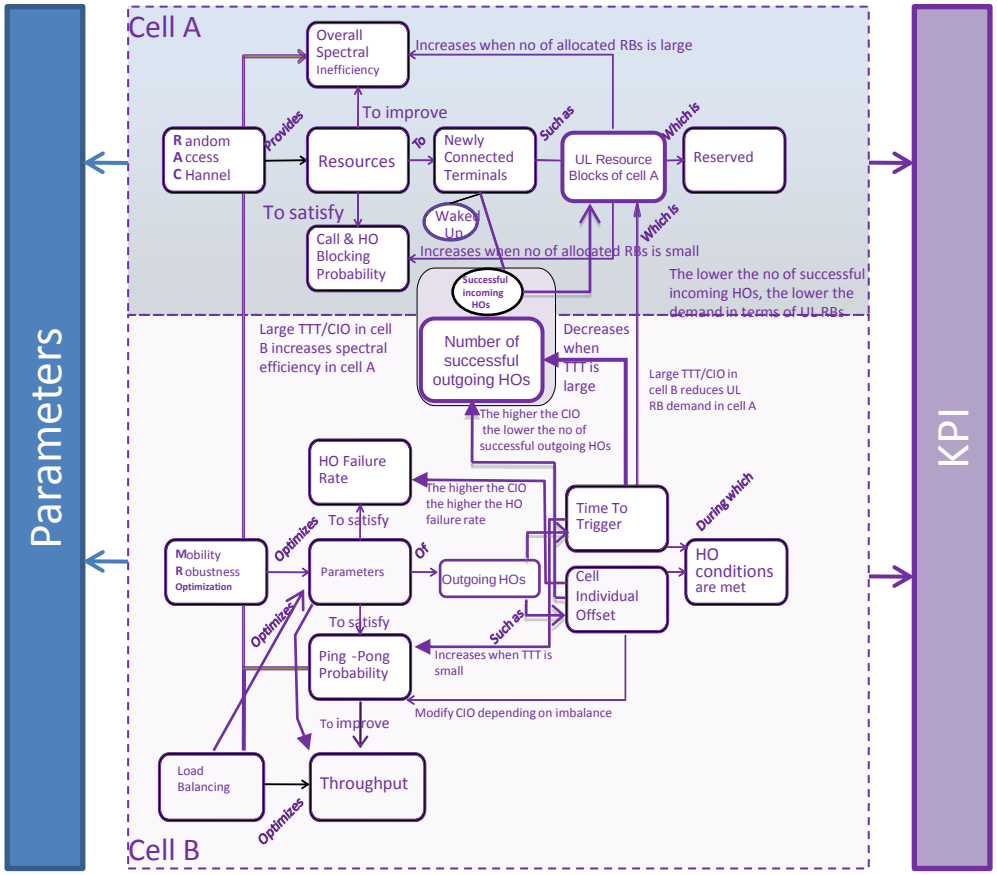
Adapted by Utility policies

Consider rather grammatical than logical meaning of a predicate:
Control Loop behaviour ~ sentence, in which Subject = CL's Decision Process

"MRO in cell A increments the TTT by 10%" = Predicate (Subject, Parameters)

Predicate (*, *) – abstract behaviour;
Predicate (S, *), Predicate (*, P) – partially qualified behaviour;
Predicate (S, P) – fully qualified behaviour

Example



No Trust | Instability | Losses | Conflicts

ETSI TR 136 902 V9.3.1 (2011-05)

Technical Report

LTE;
Evolved Universal Terrestrial Radio Access Network (E-UTRAN);
Self-configuring and self-optimizing network (SON) use cases and solutions
(3GPP TR 36.902 version 9.3.1 Release 9)

4.5 Mobility robustness optimisation

4.5.1 Use Case description

Manual setting of HO parameters in current 2G/3G systems is a time consuming task. In many cases, it is considered too costly to update the mobility parameters after the initial deployment.

For some cases, RRM in one eNB can detect problems and adjust the mobility parameters, but there are also examples where RRM in one eNB can not resolve problems:

Incorrect HO parameter settings can negatively affect user experience and wasted network resources by causing HO ping-pongs, HO failures and radio link failures (RLF). While HO failures that do not lead to RLFs are often recoverable and invisible to the user, RLFs caused by incorrect HO parameter settings have a combined impact on user experience and network resources. Therefore, the main objective of mobility robustness optimization should be reducing the number of HO-related radio link failures. Furthermore, non-optimal configuration of handover parameters, even if it does not result in RLFs, may lead to serious degradation of the service performance. Example of such a situation is incorrect setting of the HO hysteresis, which may be the reason for either ping-pong effect or prolonged connection to non-optimal cell. Thus the secondary objective will be reduction of the inefficient use of network resources due to unecessary or missed handovers.

HO-related failures can be categorized as follows:

- Failures due to too late HO triggering
- Failures due to too early HO triggering
- Failures due to HO to a wrong cell

Additionally cell-reselection parameters not aligned with HO parameters may result in unwanted handovers subsequent to connection setup, which should be avoided by parameter adjustments done by MRO function.

4.6 Mobility Load balancing optimisation

4.6.1 Use Case description

Objective:

Optimisation of cell reselection/handover parameters in order to cope with the unequal traffic load and to minimize the number of handovers and redirections needed to achieve the load balancing.

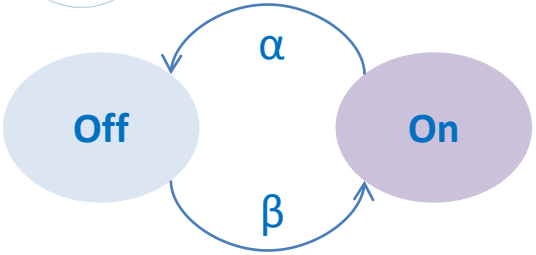
Self-optimisation of the intra-LTE and inter-RAT mobility parameters to the current load in the cell and in the adjacent cells can improve the system capacity compared to static/non-optimised cell reselection/handover parameters. Such optimisation can also minimize human intervention in the network management and optimization tasks.

The load balancing shall not affect the user QoS negatively beyond what a user would experience at normal mobility without load-balancing. Service capabilities of RATs must be taken into account, and solutions should take into account network deployments with overlay of high-capacity and low-capacity layers where high-capacity layer can have spotty coverage.

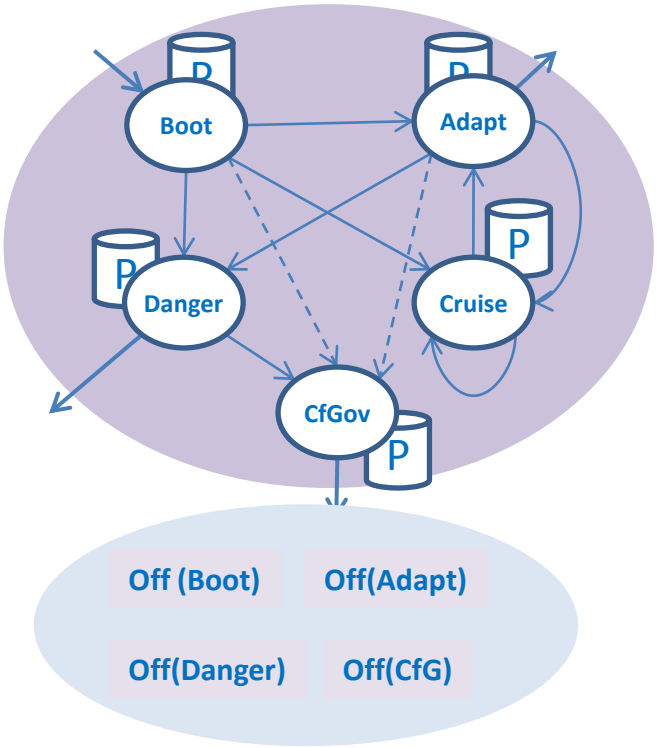
Load balancing can be done in following scenarios:

- Intra-LTE load balancing
- Inter-RAT load balancing

Towards the Design for Trust



Consider *state space* of a single Control Loop (CL)
α , β = {events | messages | inputs} generated either by goal policy or by utility policy communicated **by another CL** (subject to local decision process)



Consider *typical situations* in the On state:
Boot – resume operation of the CL:
Cruise control – normal operation (optimise the parameters);
Adapt – modify the optimisation process (also **triggered by another CL**):
Danger – anomaly detection and monitoring;
CfG – Call for Governance (request)
Label each transition with the state-specific predicate (P)
Perform transition when fully qualified, highest utility, lowest risk, …

Automatically obtain useful partitioning of the Off state:
→On next boot behave consequently

A Finite State Machine of a CL with sets of Predicates is a CL Model ;
Verified off-line, used at run-time for Governance

Design for Trust

1. Identify your control loop[s]
2. Consider state space of your CL (based on the complete life-cycle)
   21. E.g. include the state 'Call for Governance' (CfG), in which your CL shall request governance from a UMF (either when under attack/threat/failure or e.g. when local conflicts do not permit further operation)
   22. E.g. include the state 'Collaboration' (e.g. within the 'Adapt' state), in which your CL might initiate/respond a collaboration request to/from other CL
3. Consider all allowed transitions between states
4. Label each allowed transition with a predicate Pr(*, *)
   41. Include safeguards (watchdogs) to evaluate Pr(S, P) at run-time
      411. Is it on time? Is it on resource constraints? Is it in conformance with past successful behaviours? …
   42. Include Behavioural Log Files (BLF) to store information on transitions taken
   43. Include BLF ageing to keep the information only within needed time scope (might the scope be dynamic in your case?)
   44. Consider how UMF can access BLF for reading, how BLF are protected, etc.
5. Consider CL-specific Trustworthy Indicator

The Power of Predicates

- Network management automation by network empowerment is the deployment of self-managing control loops
- The CL's are self-managing within certain scope
  - The scope might be CL specific, domain specific, deployment specific, etc.
- Within the defined scope the CL must be trustworthy:
  - Predictable behvaiour of a CL → each CL is defined by its Model (known to UMF)
  - Verifiable behaviour of a CL → BLF's can be externally analysed (through the UMF)
  - Self-aware behaviour of a CL → CL Model includes CfG predicates
  - …
- Predicates are behaviour constraints that take the form of
  - Abstract behaviours at the design phase of a CL~ network and device independent config. policies
  - Partially qualified behaviours when beeing embedded in a particular network function (particular placement of network function) ~ network and device dependent config. policies
  - Fully qualified behaviours when being evaluated at run time ~ Event:Condition→Action
- The power of predicates = the power of policies
  - Can check their correctness once and recycle many times
  - Can rewrite them to cater for a new type of behaviour (but remember possible inconsistencies)

Standards Bodies Must Act on

- Certification process/model
- Conformance framework
- Metrics definition
- Predicates definition
- Test specifications
- Test procedures

UniverSelf Plans for Trust

- Identify challenges ahead for trustworthy autonomic [carrier-grade] future networks
- Detail the unified approach for management of
  - Future autonomic network technologies
  - Trust in future autonomic network
- Discuss the underlying requirements and options regarding future standardization efforts
  - Certification type
  - KPI-based envelope
  - Certification procedures
  - Business impacts
- **Actions in ETSI AFI (new work item), MTS, CTI/PlugTest**
- **Actions in IRTF/NMRG and COMPLEXITY on safe configuration detection, verification and validation**

Acknowledgments

- The research leading to these results has been performed within the UniverSelf project (www.univerself-project.eu) and received funding from the European Community's Seventh Framework Programme (FP7/2007-2013) under grant agreement n° 257513.
- The following authors contributed to this work:
  Mikhail Smirnov, Yacine Rebahi (Fraunhofer FOKUS)
  Imen Grida Ben Yahia, Christian Destré, Berna Sayrac (Orange Labs)
  Evaggelos Kosmatos, Eleni Patouni (NKUA)
  Beatriz Fuentes, Alfonso Castro (Telefónica I+D)
  Samir Ghamri-Doudane, Laurent Ciavaglia (Alcatel-Lucent Bell Labs).

THANK YOU!

FOLLOW US IN FIA POZNAN SESSION ON TRUST FRAMEWORK FOR SERVICES AND INFRASTRUCTURES

References

1. 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. Yacine Rebahi, Ranganai Chaparadza, "EFIPSANS Security Roadmap", EU FP7 EFIPSANS project
3. Pedro B. Velloso, Laurent Ciavaglia "Composition of Well-known Metrics to Characterize Autonomic Networks", IEEE Network Magazine
4. Paulo Esteves Verissimo "Thou Shalt Not Trust non-Trustworthy Systems", Keynote at the Workshop on Assurance in Distributed Systems and Networks (ADSN2006), with the 26th IEEE International Conference on Distributed Computing Systems (ICDCS 2006), Lisboa, Portugal, July 2006
5. R. de Lemos, J.A. McCann, O. F. Rana, A. Wombacher, M. Huebscher, "Academic Panel: Can Self-Managed Systems Be Trusted?", Sixteenth International Workshop on Database and Expert Systems Applications, 2005.
6. Thomas Hirsch, Fraunhofer FOKUS, *Distributed Cooperation Models for Autonomic Organisation*, OKS AC Conference proceedings, 2006
7. ETSI TR 136 902 V9.3.1 (2011-05) LTE; Evolved Universal Terrestrial Radio Access Network (E-UTRAN); Self-configuring and self-optimizing network (SON) use cases and solutions (3GPP TR 36.902 version 9.3.1 Release 9)

Glossary

- **Trust** - believe: be confident about something [Wordnet]
- **Autonomic** - Acting or occurring involuntarily; automatic: an autonomic reflex [IBM]
- **Certification** - the confirmation of certain characteristics of an object, person, or organization … often … provided by assessment. … [Wikipedia]
- **Assessment** - Is concerned with the process (behaviour) observation, in which observation the competence of the process (behaviour) is related to the given purpose. Assessment verifies the behaviour in that it is correct *'both in the sense of responding appropriately to changes in context and in the sense of continuing to meet the high-level requirements of the system*' [ACF, S.Dobson];
  evaluation of learning related to the purpose [E3 Glossary]
- **Correctness** ~ conformance to spec [Wikipedia] or rather "having the right opinion„ [Greek] ? ← belief