

# THALES



## Towards Mission Critical Support in 5G slicing

Emmanuel Dotaro

Head of ICT & Security Labs

Thales Secure Communications and Information Systems

Bologna, July 2017

[www.thalesgroup.com](http://www.thalesgroup.com)

OPEN



Is there a need ?

5G  
for Verticals  
supporting "Mission Critical"

requires adequate **RESILIENCE** and a bit of **SECURITY**

[not only "as usual"]

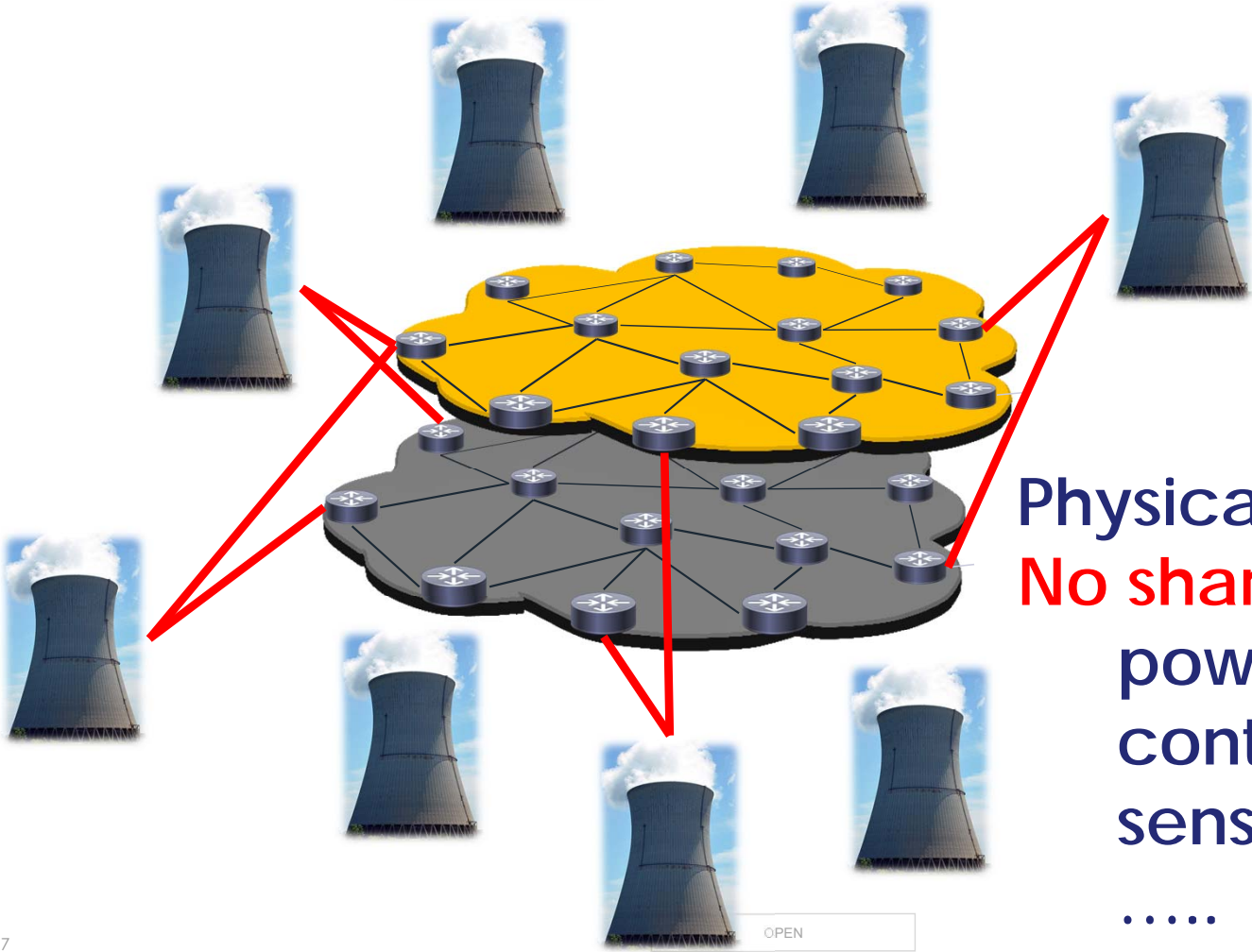
[confidentiality]

[integrity]

[availability]

[tech/arch/biz/societal]

# What critical really means...



**Physical disjointness**  
**No shared risk**  
power supply  
control/NOCs  
sensitivity to attacks

.....



This document may not be reproduced, modified, adapted, published, translated, in any way, in whole or in part or disclosed to a third party without the prior written consent of Thales - © Thales 2015 All rights reserved.

OPEN

# About 5G slices...



Operator or virtual operator

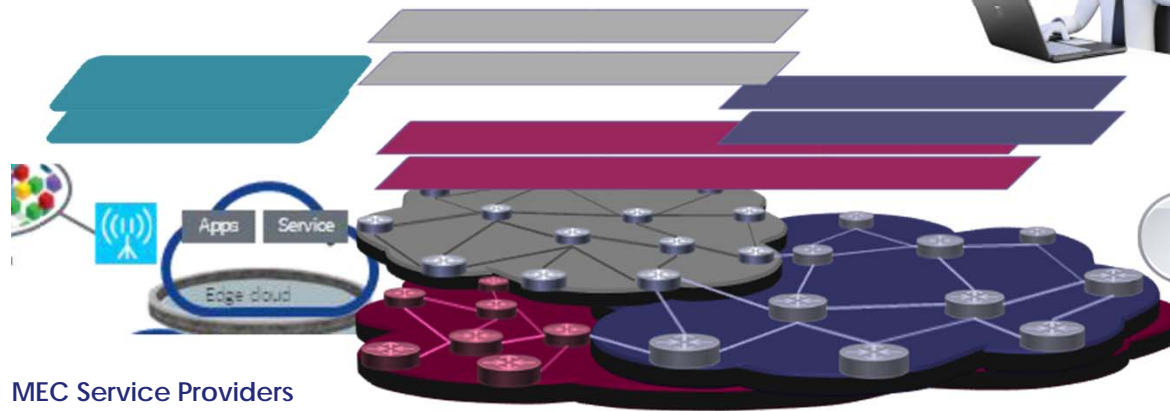
Tenant slice as  
« virtual Infrastructure »



(other) Service Providers



Cloud Service Providers



MEC Service Providers

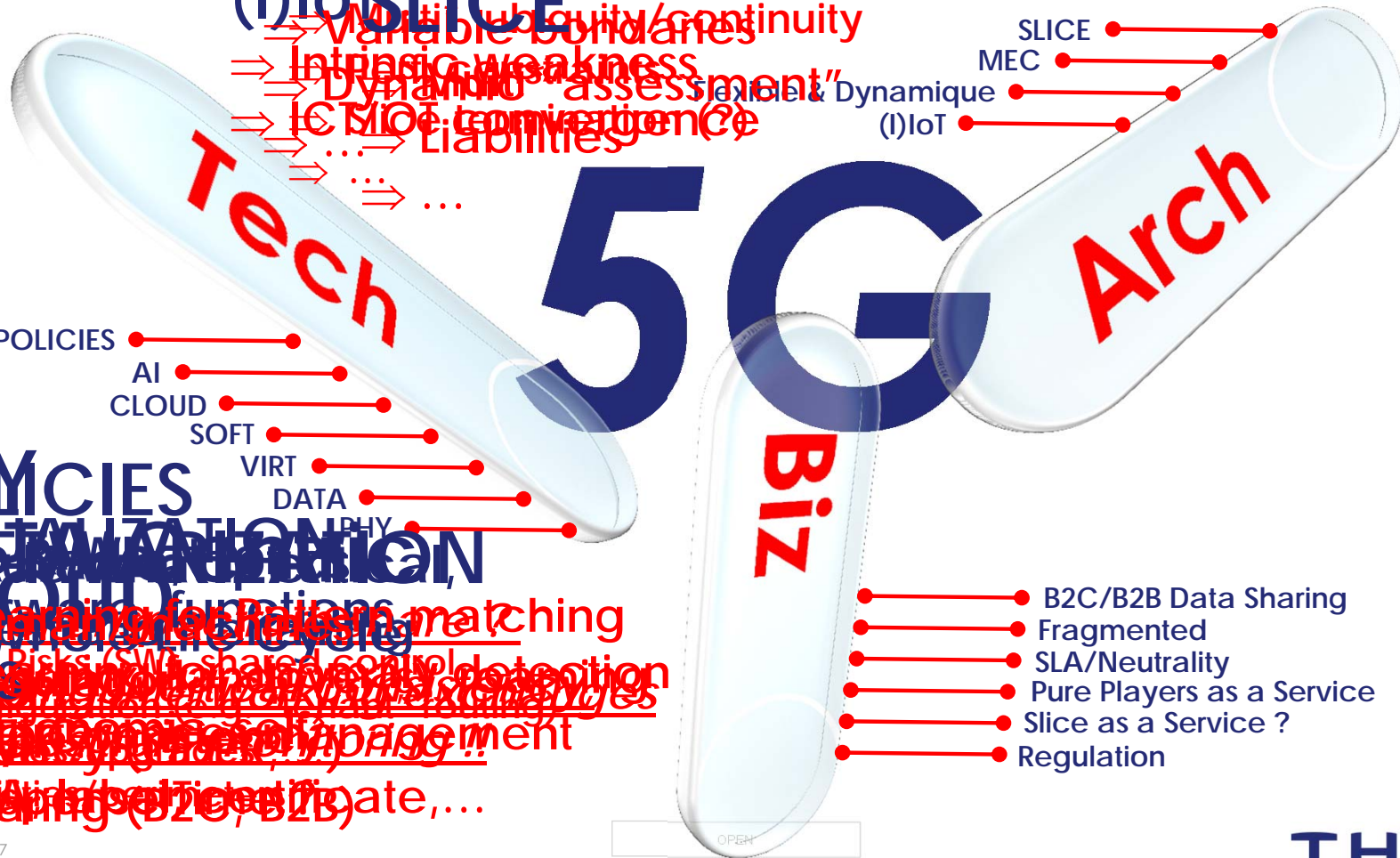
Network Service Providers

OPEN

THALES

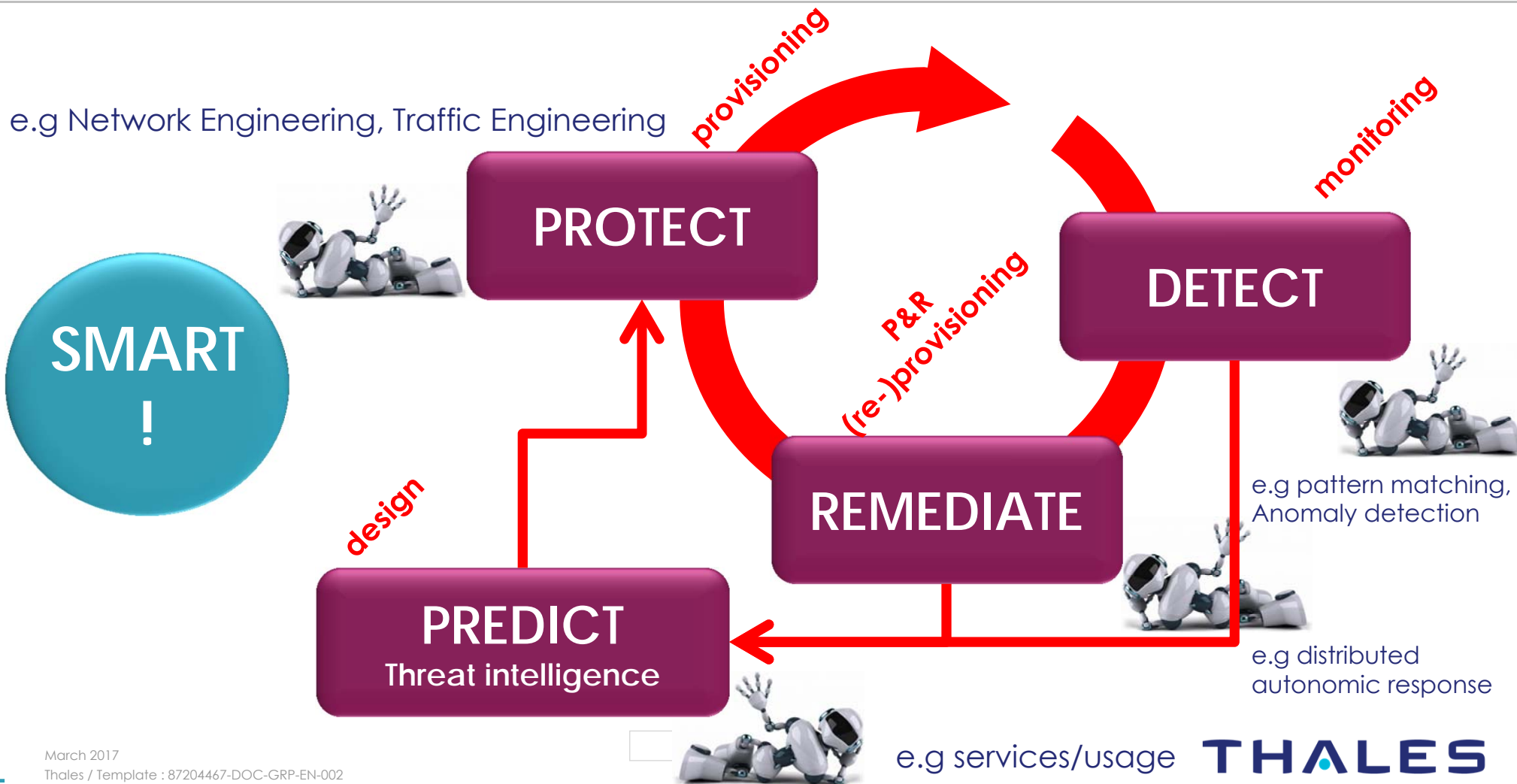
# A multi-factors, complex 5G eco-system

## MEGAMORPHIC SYSTEMS



# Where AI stands: Safety, Security, Reliability convergence

e.g Network Engineering, Traffic Engineering



This document may not be reproduced, modified, adapted, published, translated, in any way, in whole or in part or disclosed to a third party without the prior written consent of Thales - © Thales 2015 All rights reserved.

# There is a « but », there are still many gaps !

## In essence 5G is a multi-lateral complex system

### Lack of:

- Vertical integration (tenants over recursive control perimeters)
- Horizontal integration (E2E !!)
- But also other third-parties (MSSPs, CSPs,...)

### Need of sharing of:

- Who's in charge of what: TENANTS – PROVIDERS / PROVIDERS-PROVIDERS
  - Service provisioning phase (including respective SLA/policies)
  - Configuration/updates/upgrades phase (a kind of permanent transient state)
  - Monitoring (failure, degradation, attacks)
  - Response/remediation coordination (triggers, states, notifications,...)

OPEN

**THALES**

# Critical often means deterministic & Real Time

## Some questions/challenges as food for thoughts

- Can we abstract everything in the service interworking (instead of ctl, mgt,...)
- How to adapt optimal distribution of response provisioning
  - Data/control/management/service among the various perimeters
- How to differentiate mission Critical support from best effort
  - Without being blocked by « net neutrality »
  - Introducing precedence paradigm at service level ?
- As well known multi-layer issues: is there a mandate for explicit notification ?
  - Can't support cascade of Hold of timers
- AI-based mechanisms
  - available data ?
  - How many control loops !!

OPEN

THALES



## conclusion

# One size fit all ?

### *Some Directions:*

- **B2C/B2B relations in 5G mandates interoperability in terms of specific resiliency attributes:**
  - Service exposure
  - Service negotiation
  - Service monitoring
  - Explicit notification (vertical & horizontal bounds)
  - Secure all of that !
  
- **AI**
  - Learning when relevant data available
  - Distributed Autonomic adaptive approaches under global consistency
  - But also code morphology

# THALES

Thanks

[www.thalesgroup.com](http://www.thalesgroup.com)

OPEN



