Model-Driven Analysis of Security, Reliability, Test, Privacy, Safety and Trust of IoE Services

Eugenio Villar
University of Cantabria

Agenda

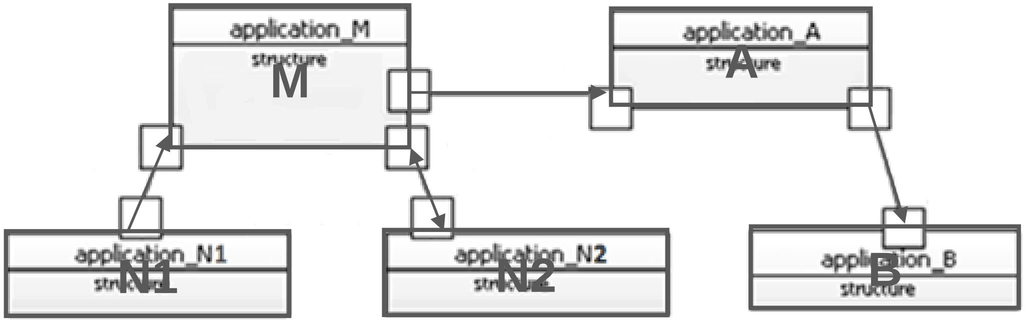
- Introduction
- Single-Source Embedded Systems Design
- Model-driven Analysis of IoE Services
- Conclusions

Introduction

- Model-Driven Design (MDD)
  - High-abstraction level
  - Mature SW engineering methodology
- State-of-the-Art
  - Matlab-Simulink
    - Proprietary, only one MoC, M language
  - CoFluent
    - Proprietary, a few MoCs, C/C++ language
  - Ptolemy II
    - Academic, any MoC, C/C++ inside a Java block
  - …

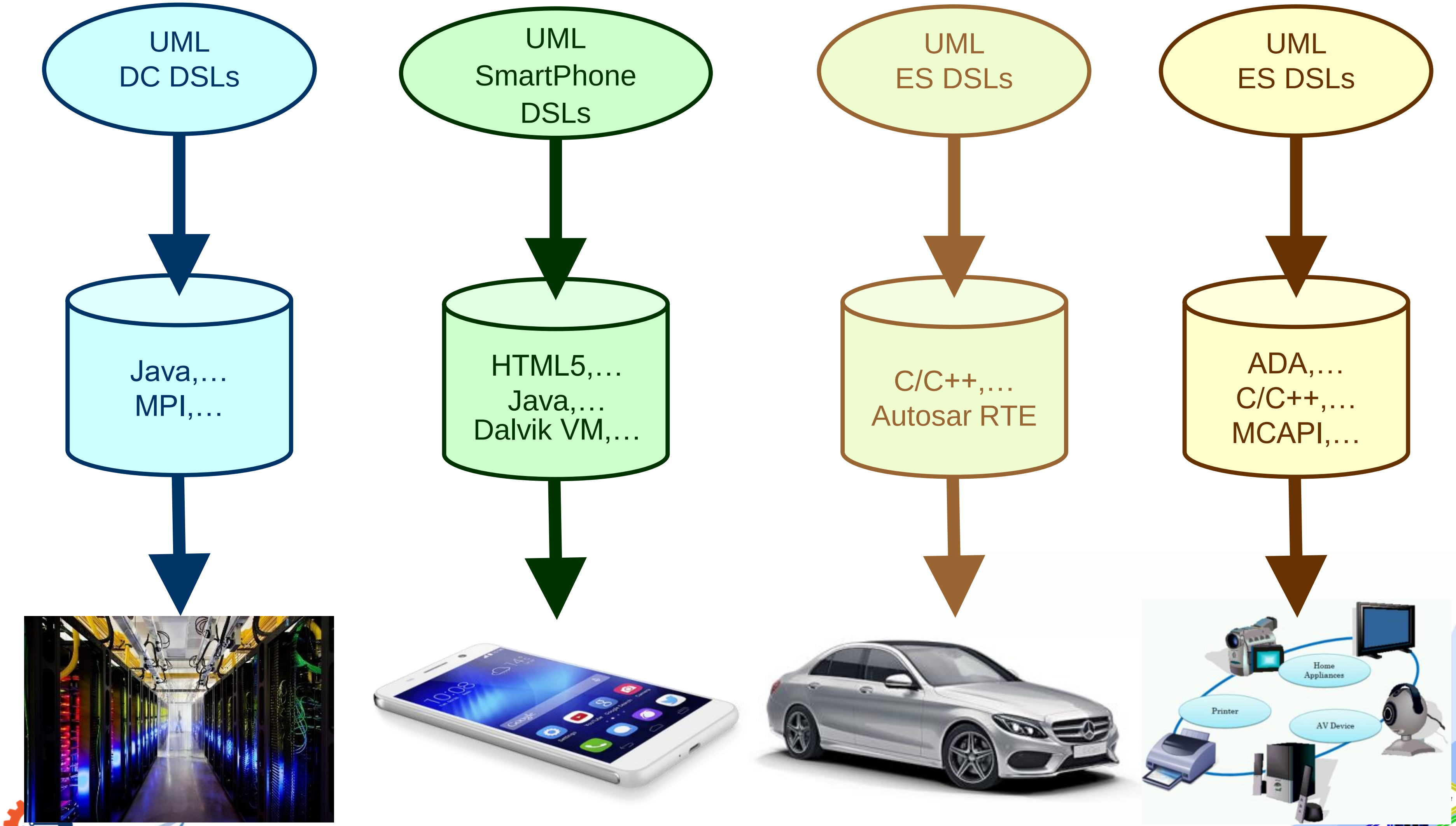
Introduction

- UML
  - Standard, any (user-defined) MoC, any language
  - Natural way to capture system architecture



- Semantic lacks
- Domain-specific profiles
- MetaMorph
  - Commercial, any (user-defined) MoC, language agnostic
- CHESS
  - Open Source, any (user-defined) MoC, language agnostic

Introduction



UML
DC DSLs

Java,…
MPI,…

UML
SmartPhone
DSLs

HTML5,…
Java,…
Dalvik VM,…

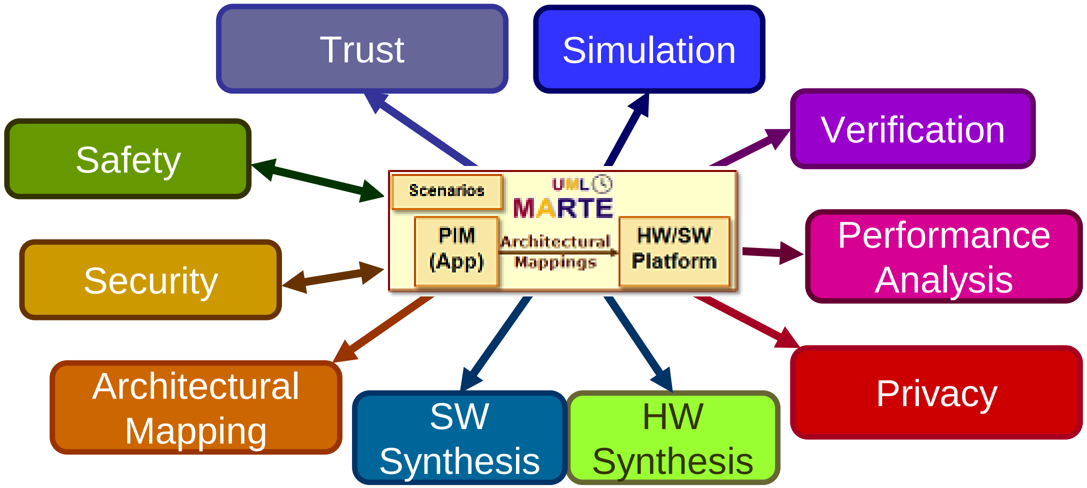
UML
ES DSLs

C/C++,…
Autosar RTE

UML
ES DSLs

ADA,…
C/C++,…
MCAPI,…

Single-Source Embedded System Design



Trust

Simulation

Verification

Safety

Security

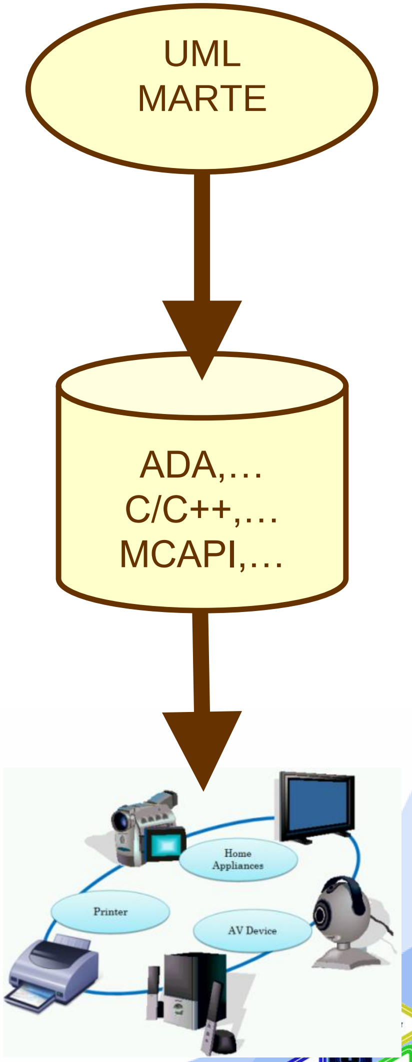
Performance Analysis

Privacy

Architectural Mapping

SW Synthesis

HW Synthesis

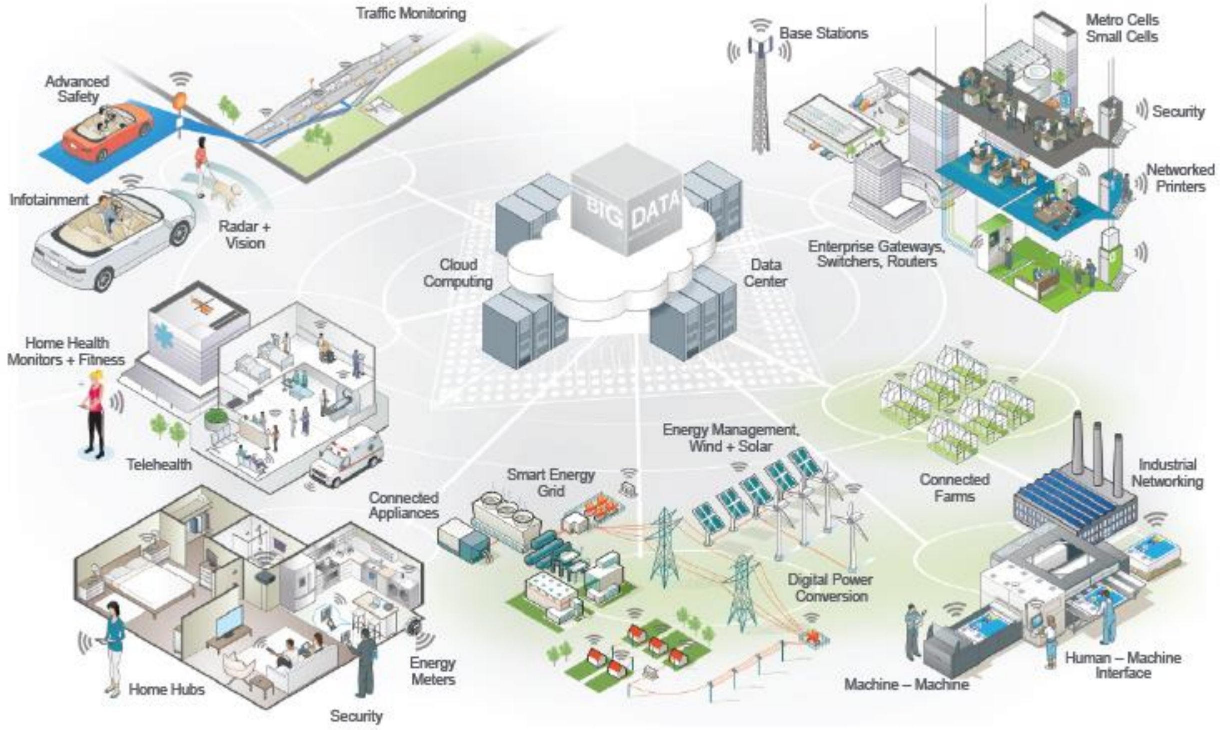


UML MARTE

ADA,…
C/C++,…
MCAPI,…

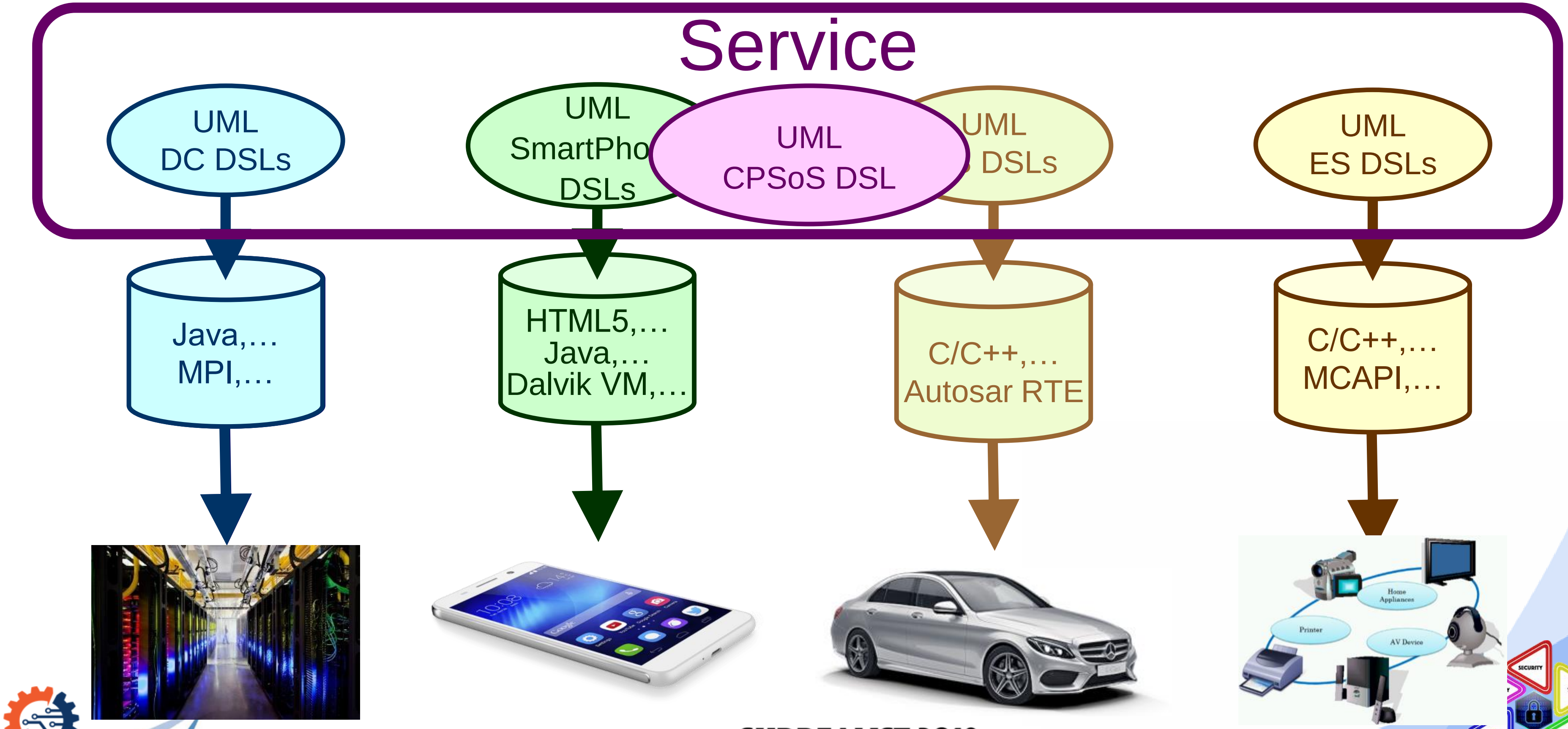
Model-Driven Analysis of IoE Services

- Programming the Internet of Everything
- Services provided on computing platforms of many kind



Model-Driven Analysis of IoE Services

- Programming the Internet of Everything
- Services provided on computing platforms of many kind



Service

UML
DC DSLs

UML
SmartPho
DSLs

UML
CPSoS DSL

UML
DSLs

UML
ES DSLs

Java,…
MPI,…

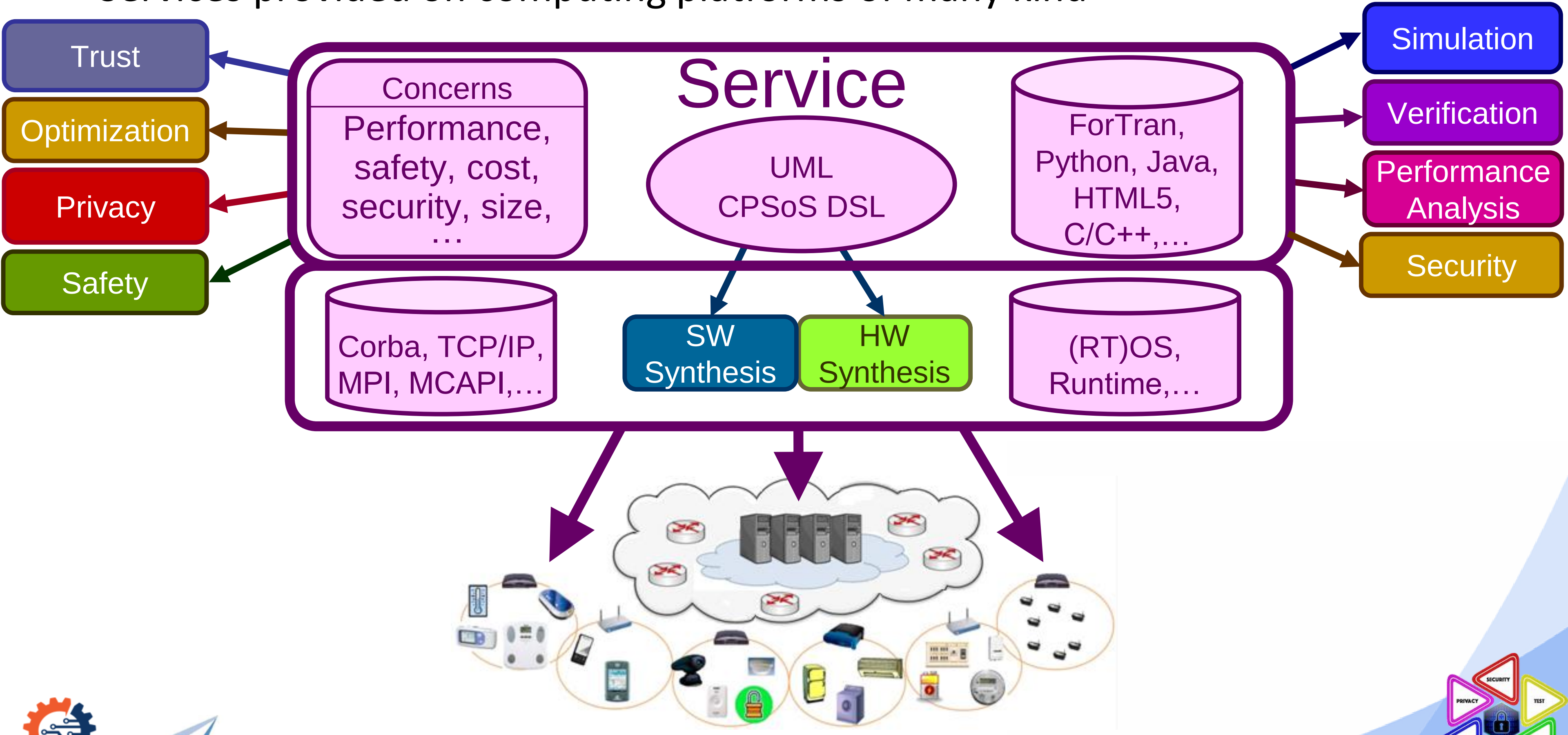
HTML5,…
Java,…
Dalvik VM,…

C/C++,…
Autosar RTE

C/C++,…
MCAPI,…

Model-Driven Analysis of IoE Services

- Programming the Internet of Everything
- Services provided on computing platforms of many kind



Trust

Optimization

Privacy

Safety

Service

Concerns

Performance, safety, cost, security, size, …

UML
CPSoS DSL

ForTran, Python, Java, HTML5, C/C++,…

Simulation

Verification

Performance Analysis

Security

Corba, TCP/IP, MPI, MCAPI,…

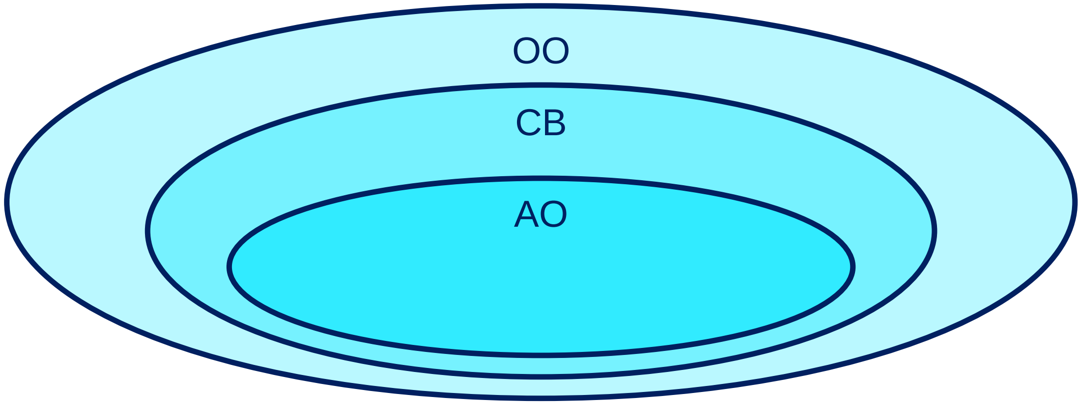
SW Synthesis

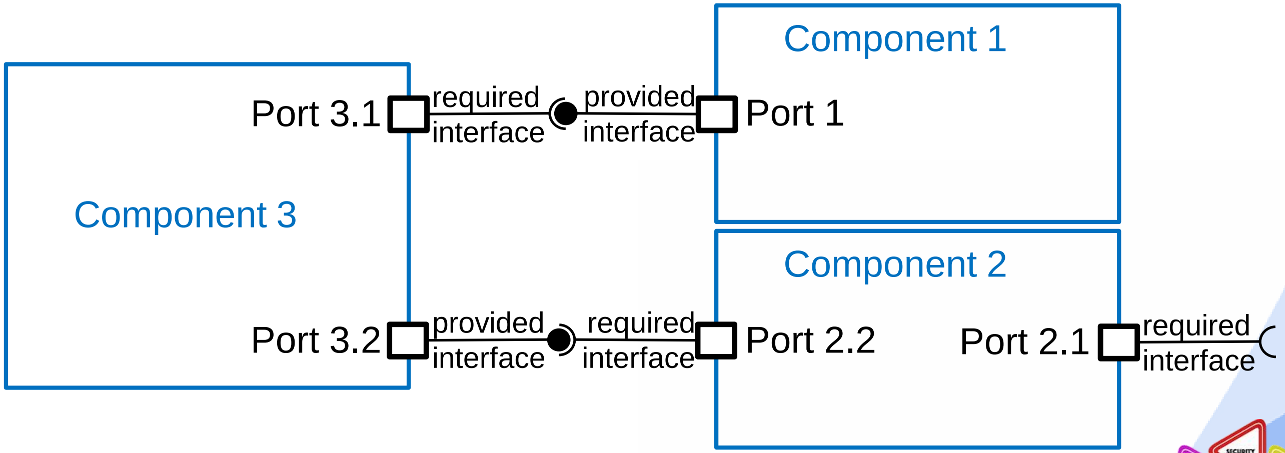
HW Synthesis

(RT)OS, Runtime,…

Model-Driven Analysis of IoE Services

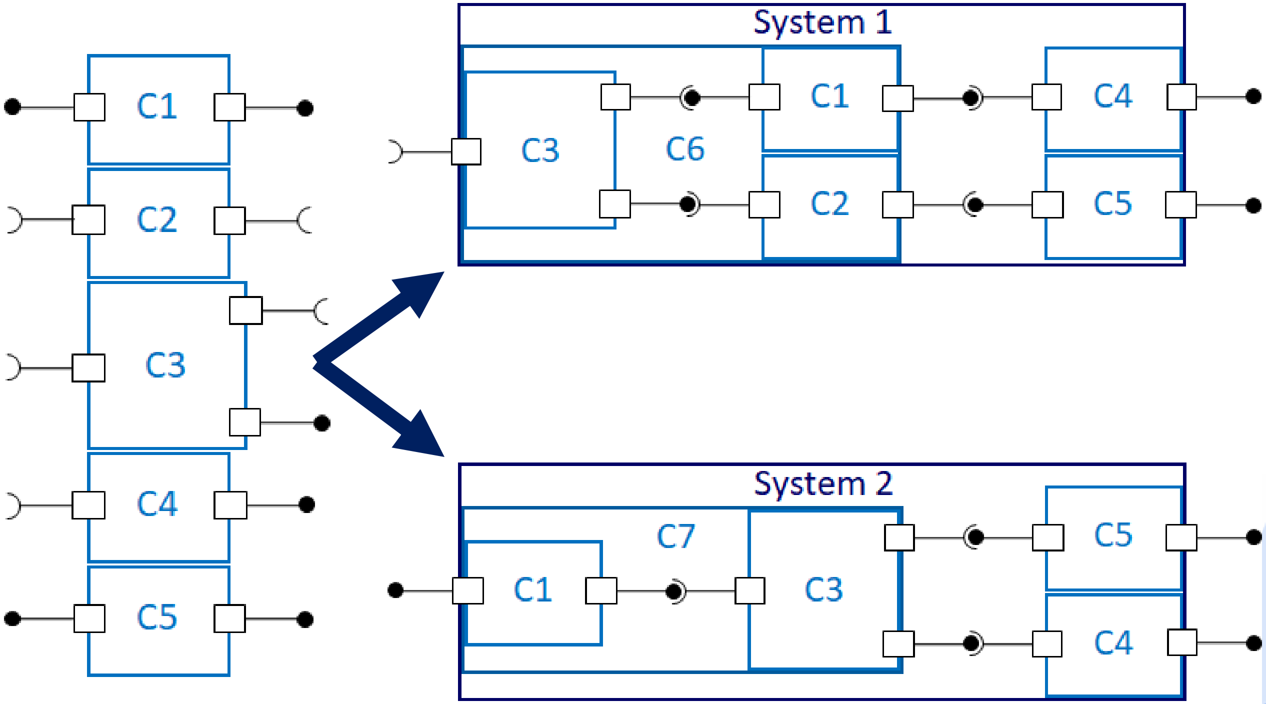
- UML/MARTE System Modeling Methodology
- Platform-Independent
- Component-Based
  - Supporting
    - Object-Orientation
    - Actor-Orientation





Model-Driven Analysis of IoE Services

- UML/MARTE System Modeling Methodology
- Platform-Independent
- Component-Based
  - Supporting
    - Object-Orientation
    - Actor-Orientation
- Reusable
- Flexible
- Analyzable
  - Security
  - Reliability
  - Test
  - Safety
  - Privacy, Trust…



Model-Driven Analysis of IoE Services

- Properties of the Provided Port
  - NotAttendedService
  - Retry
- Properties of the Interface Methods
  - concurrency
  - exekind
  - syncKind
- Properties of the Required Port
  - queueSize
  - FullPoolPolicy

Model-Driven Analysis of IoE Services

- Function Call/RPC/RMI

Required Port		RtService			Provided Port		MoC
NotAttendedService	retry	concurrency	exekind	syncKind	queueSize	FullPoolPolicy	
infiniteWait	none	G or C	rem.Im.	sync.	none	none	exactly once
infiniteWait	none	G or C	rem.Im.	async.	none	none	at most once
dynamic	none	G or C	rem.Im.	sync.	none	none	exactly once
dynamic	none	G or C	rem.Im.	async.	none	none	at most once
timedWait	0	G or C	rem.Im.	sync.	none	none	exactly once
timedWait	0	G or C	rem.Im.	async.	none	none	at most once
timedWait	> 0	G or C	rem.Im.	sync.	none	none	at least once
timedWait	> 0	G or C	rem.Im.	async.	none	none	maybe once

- Rendezvous

Required Port		RtService			Provided Port		MoC
NotAttendedService	retry	concurrency	exekind	syncKind	queueSize	FullPoolPolicy	
infiniteWait	none	G or C	rem.Im.	rendezvous	none	none	CSP
timedWait	0	G or C	rem.Im.	rendezvous	none	none	RV
timedWait	> 0	G or C	rem.Im.	rendezvous	none	none	RV

Model-Driven Analysis of IoE Services

- Data-Flow

Required Port		RtService			Provided Port		MoC
NotAttendedService	retry	concurrency	exekind	syncKind	queueSize	FullPoolPolicy	
infiniteWait	none	G or C	deferred	async.	> 0	block	KPN/SDF
infiniteWait	none	G or C	deferred	async.	> 0	(any other)	DF
dynamic	none	G or C	deferred	async.	> 0	any	DF
timedWait	0	G or C	deferred	async.	> 0	any	DF
timedWait	> 0	G or C	deferred	async.	> 0	any	DF

- Discrete-Event/Time-Triggered/Timed Data-Flow

Required Port		RtService			Provided Port		MoC
NotAttendedService	retry	concurrency	exekind	syncKind	queueSize	FullPoolPolicy	
dynamic	none	G or C	rem.Im.	async.	none	none	DE/TT/TDF

Conclusions

- The IoE demands new CPSoS design methods and tools
- Model-Driven system design is a powerful candidate
  - A CPSoS system modeling language is required
  - Supporting Mega-Modeling
  - Analysis & design of the whole IoE service
- Single-Source Approach